



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/678,333	10/03/2003	Bryan Stephenson	200310100-1	2561

22879 7590 12/10/2010
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS, CO 80528

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2432

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

12/10/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
ipa.mail@hp.com
laura.m.clark@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BRYAN STEPHENSON

Appeal 2009-008136
Application 10/678,333
Technology Center 2400

Before KENNETH W. HAIRSTON, ELENI MANTIS MERCADER,
and CARL W. WHITEHEAD, JR., *Administrative Patent Judges*.

HAIRSTON, *Administrative Patent Judge*.

DECISION ON APPEAL¹

¹ The two-month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, or for filing a request for rehearing, as recited in 37 C.F.R. § 41.52, begins to run from the “MAIL DATE” (paper delivery mode) or the “NOTIFICATION DATE” (electronic delivery mode) shown on the PTOL-90A cover letter attached to this decision.

This is an appeal under 35 U.S.C. §§ 6(b) and 134 from the final rejection of claims 1 to 33. After submission of the Appeal Brief, the Examiner allowed claims 12 to 22, and objected to claims 6 to 10 and 28 to 32 as being dependent upon rejected base claims, but would be allowable if rewritten in independent form including all of the limitations of the base claims and any intervening claims (Ans. 2). Accordingly, claims 1 to 5, 11, 23 to 27, and 33 remain before us on appeal. We will affirm.

The disclosed invention relates to a method and system for automatically mitigating damage to a network of computing resources by isolating a remotely located computing resource in the network when it receives an unauthorized intrusion (Fig. 4; Spec. 4, 16-21; Abstract).

Claim 1 is representative of the claims on appeal, and it reads as follows:

1. A method for responding to network intrusions, comprising:
 - a) receiving an intrusion detection system (IDS) alert from an IDS sensor located in a network of computing resources, wherein said IDS alert indicates an unauthorized intrusion upon a remotely located computing resource in said network of computing resources;
 - b) identifying said IDS alert; and
 - c) determining an appropriate response to said IDS alert that is identified at a location separate from said remotely located computing resource so that said determining said appropriate response is unaffected by said unauthorized intrusion; and
 - d) automatically implementing said appropriate response to mitigate damage to said network of computing resources from said unauthorized intrusion by isolating said remotely located computing resource.

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Talpade

US 2004/0148520 A1

Jul. 29, 2004

The Examiner rejected claims 1 to 5, 11, 23 to 27, and 33 under 35 U.S.C. § 102(e) based upon the teachings of Talpade.

Appellant argues (App. Br. 9) that Talpade does not teach “protecting assets within the customer’s network regardless of the source of the attacks, and in particular protecting against attacks originating from within the customer’s network.” Appellant’s argument does not point to any error committed by the Examiner because such an argument is not commensurate in scope with the claimed invention.

Appellant argues (App. Br. 9) that “Talpade teaches away from ‘isolating said remotely located computing resource.’”

Thus, we have to determine whether Talpade teaches away from “isolating said remotely located computing resource.”

According to the Examiner

[A] careful reading of Talpade reveals that such feature/limitation is indeed taught at the passage cited in the rejection of the claims in the final office action.

For instance, Talpade at least on the abstract discloses the following. “Service attacks, such as denial of service and distributed denial of service attacks, of a customer network are detected and subsequently mitigated by the Internet Service Provider (ISP) that services the customer network. A sensor examines the traffic entering the customer network for attack traffic. When an attack is detected, the sensor notifies an analysis engine within the ISP network to mitigate the attack. The analysis engine configures a filter router to advertise new routing information to the border and edge routers of the ISP network. The new routing information instructs the border and edge routers to reroute attack traffic and non-attack traffic destined for the customer network to the filter router. At the filter router, the attack traffic and non-attack traffic are automatically filtered to remove the attack traffic. The non-attack traffic is passed back

onto the ISP network for routing towards the customer network” and this meets the following limitation, “automatically implementing said appropriate response to mitigate damage to said network of computing resources from said unauthorized intrusion, by isolating said remotely located computing resource[.]”

(Ans. 10).

Inasmuch as the claims on appeal do not preclude re-routing non-attack traffic back to the remotely located computing resource after the attack traffic is filtered by “isolating said remotely located computing resource,” we agree with the Examiner’s findings and analysis.

In summary, the anticipation rejection of claims 1 to 5, 11, 23 to 27, and 33 is sustained because: the Examiner did not err by finding that Talpade teaches “isolating said remotely located computing resource” during the filtering of the attack traffic; and each and every limitation in the claims is found either expressly or inherently in the cited reference to Talpade. *In re Crish*, 393 F.3d 1253, 1256 (Fed. Cir. 2004).

The decision of the Examiner is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(v).

AFFIRMED

babc

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
3404 E. Harmony Road
Mail Stop 35
FORT COLLINS CO 80528